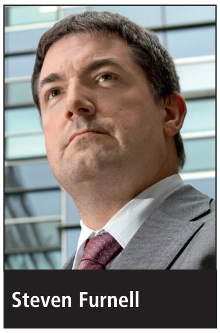
Home working and cyber security – an outbreak of unpreparedness?



Steven Furnell

Steven Furnell, School of Computer Science, University of Nottingham and Jayesh Navin Shah, Ipsos MORI

Home working has been one of the long-promised freedoms of information technology. But until recently it was something that relatively few people had routinely experienced in practice (aside, perhaps, from taking work home to do in the evenings and at weekends). This situation abruptly changed in early 2020, with the Covid-19 pandemic forcing organisations to shut their doors and send staff home. Across the globe, home working wherever possible became the standard advice, and technology was the fundamental enabler of the change.

Home working is by no means a new concept, but equally it is not a context in which security has been a frequent priority. Indeed, examining the situation back in 2006 revealed some clear shortcomings in terms of user awareness and safeguards, which combined to leave them less than well-prepared in the context of home working.[1] It is therefore interesting to consider whether – more than a decade later – things have changed, and in particular whether sufficient provisions were in place when they were suddenly and unexpectedly needed.

> ***"The 10 steps are intended to provide recommendations that span the breadth of cyber security and cover the key areas that safeguard organisations from attacks and breaches. However, the extent to which businesses are actually compliant with them is rather variable"***

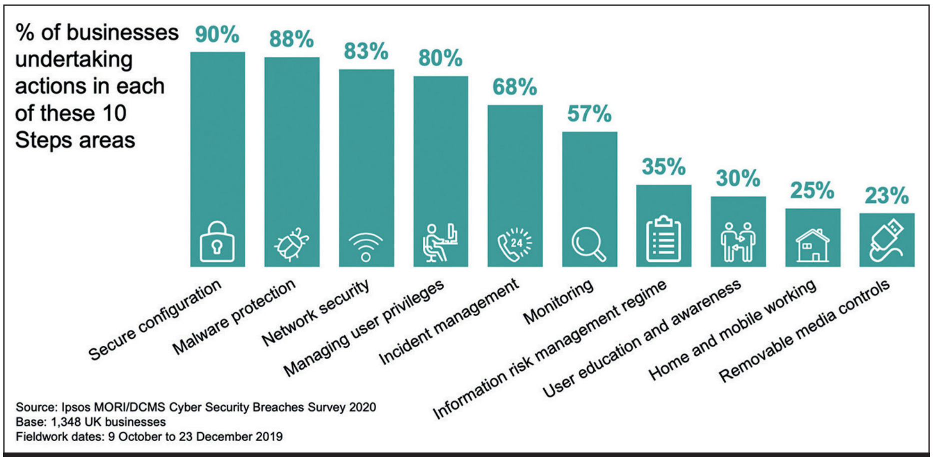
Secured or otherwise, home working has also not been the norm for a large proportion of the workforce. As an example, on 16 March 2020 (a week before the commencement of lockdown in the UK), only 15% of UK employees were working at home. However, this figure had more than doubled within the following month, reaching 38% by April 13.[2] Applying this percentage increase to base employment data from the Office for National Statistics suggests approximately an additional 6.8 million employees working at home at the peak of lockdown.[3]

This article examines the extent to which organisations and their staff were likely to have been prepared for the unplanned outbreak of home working, along with the increased cyberthreats that were faced in parallel. It should be noted that while the discussion takes a fairly UK-focused perspective on the issue (due to the key data sources available to the authors), the overall picture in other regions is likely to be similar, in terms of both prior preparedness and implications for the future.

Prior preparedness

Drawing on data from the UK Cyber Security Breaches Survey (CSBS) 2020, Figure 1 examines businesses' prior attention to actions that map into the different recommendations from the National Cyber Security Centre's '10 Steps to Cyber Security'.[4,5] Originally established in 2012, the 10 steps are intended to provide recommendations that span the breadth of cyber security and cover the key areas that safeguard organisations from attacks and breaches. However, the extent to which businesses are actually compliant with them is rather variable, with 12% of businesses having undertaken action against all 10 steps.

This proportion does increase according to the size of the organisation, rising from



Source: Ipsos MORI/DCMS Cyber Security Breaches Survey 2020
Base: 1,348 UK businesses
Fieldwork dates: 9 October to 23 December 2019

Figure 1: Businesses' claimed compliance with the '10 Steps to Cyber Security'.

9% in micro firms with 1-9 employees, through to 42% in large firms with 250+ employees. Larger firms would naturally be expected to have the skills and resources to do better at each of the 10 steps than smaller organisations. Larger firms also tend to have more complex cyber security needs, so often need to do more – the vast majority of small businesses do not necessarily need advanced network security or monitoring tools. Nevertheless, the 10 steps still provide a comprehensive framework for cyber security for organisations of all sizes and help us to see in which aspects of cyber security organisations have invested.

Looking at a more granular level and considering the compliance with each of the 10 steps, it is clear that the vast majority of firms appear to be attending to the technology-related aspects of security, but there is a notable drop-off in relation to those aspects that are more business-, policy- and people-centric (a picture that has remained essentially unchanged across all instances of the survey, since the first release in 2016). For example, the results depicted in the chart clearly suggest a lack of attention to the steps around the category of 'Home and mobile working and user education and awareness', with only a quarter to a third of businesses claiming to have addressed them.

Underlying findings

To unpack what these results actually mean, it is relevant to consider the underlying survey findings that contribute to them:

- **Home and mobile working** refers to the percentage of businesses that have a formal policy on cyber security that explicitly covers home and mobile working. Other organisations may have rules around this that are laid out elsewhere (ie, not in the cyber security policy) and others may have unwritten rules or rely on common sense. But what this finding suggests is that in three-quarters (75%) of businesses, there are no explicit *cyber security-framed, written* rules that staff are expected to follow when working at home.
- **User education and awareness** refers to the percentage of businesses that have a formal policy on cyber security that explicitly covers what staff are permitted to do on the organisation's devices (ie, the percentage of organisations that have documented acceptable staff behaviour somewhere and don't just leave it to common sense). It notably does not include staff training, as the CSBS no longer measures this issue. However, other research shows that this is also highly uncommon across the whole UK business population, with only 1 in 9 businesses (11%) having provided cyber security training to non-cyber employees in the past year.[6]

The fact that the picture is essentially unchanged over time suggests that organisations are either feeling untroubled by these aspects or have not learned the lessons of prior incidents. The results relating to home and mobile working are potentially linked to the low prevalence of home working across UK businesses up to this point: with so few employees doing it on a regular basis, the risk was perhaps not considered worth mitigating. Some indirect supporting evidence here is the fact that there have historically been more charities than businesses with home working in their cyber policies (29% vs. 25% in CSBS 2020). It reflects the fact that charities have tended to have more people who work from home and use personal devices, because they are less able to afford bespoke office space and equipment.[7] With the current increase in home working, businesses may now start to take these risks a lot more seriously and become more interested in seeking out guidance on home working.

Unlearned lessons

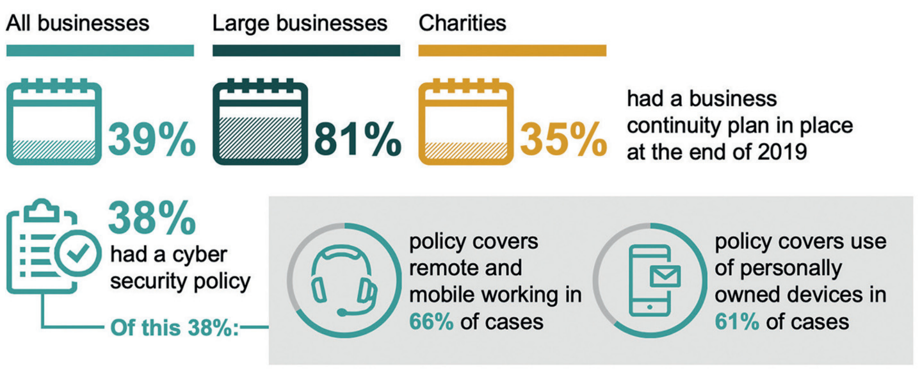
Unfortunately, there is also evidence to support the view that lessons have not been learned. For example, further findings from CSBS 2020 indicate that the most common action taken in response to the most disruptive breaches or attacks is "additional staff training or communication". This would seem to suggest that training is often needed, but the support is not being provided proactively. In fact, previous findings from the CSBS series more generally have tended to suggest three potential schools of thought among those in charge of cyber security:

- Those that recognise the importance of end user awareness and who feel that their main challenge is often convincing management boards or securing budgets for end user training and awareness raising.
- Those who expect the worst from end users and whose primary approach is typically to remove as much control from them as possible and lock down their systems.
- Those that treat cyber security as an issue of common sense, where end users just need to take sensible precautions, which do not necessarily need to be written down or delivered through training – anecdotally a less common view in more recent years of the study.

> ***"If home working increasingly becomes the new normal then it makes it impossible to lock everything down or rely solely on the common sense of employees. As such, it makes user awareness imperative"***

The upshot is that, in spite of the clear people-related problem, there is often an unfortunate tendency for security awareness and education to be dismissed as a "waste of time".[8] The consequent inaction is then frequently excused on the assumption or assertion that people will not take any notice, and that it will not make any difference.

While such beliefs may prove to be true in some cases, having it as a general assumption serves to paint a negative



Source: Ipsos MORI/DCMS Cyber Security Breaches Survey 2020
Bases: 1,348 UK businesses; 213 large firms; 337 charities
Fieldwork dates: 9 October to 23 December 2019

Figure 2: Preparedness for home working among UK businesses and charities.

and potentially unfair picture of the staff base as a whole, and can result in staff being denied support as a result. It also leaves a fundamental question for the organisation: why should we expect staff to understand and use security effectively, or exhibit security-aware behaviours if we have not supported them to do so? Moreover, if home working increasingly becomes the new normal then it makes it impossible to lock everything down or rely solely on the common sense of employees. As such, it makes user awareness imperative.

Looking more specifically at the data from the most recent release of the 'Cyber Security Breaches Survey' (the fieldwork for which was conducted in the fourth quarter of 2019, just before Covid-19 was first reported), Figure 2 looks at the preparedness in terms of policies and plans. We can see that organisations as a whole were notably lacking in their overall positioning, with further patchiness in the underlying attention to the specifics of remote working and use of personal devices (both of which, of course, become areas of increased dependency in the context of enforced home working).

Taking security home with us?

What the data also suggests is that staff in many organisations are likely to have been unprepared for a sudden and unexpected transition to home working. As in many other contexts, staff could find that they have been given the tools (eg, taking their laptops and/or other devices home), but not the training. As such, many workers will have essentially found themselves being asked to work from home with only their experience of personal IT usage to guide them. And to illustrate what this experience may amount to in terms of security, prior research had found that only 15% of the general public claimed to know "a great deal" about how to protect themselves from harmful cyber activity. Meanwhile, 23% said they knew "not very much" and 7% said they knew "nothing".[9]

Historically, there was often little expectation of home users adopting security of their of own volition, and it was seen as something that could actively be a disincentive for them in using technology. This is well illustrated by the following quote from one of Microsoft's senor technology specialists back in 2000, contemplating the potential for home users to adopt the latest version of Windows: "I don't expect a lot of consumers to adopt Windows 2000 because, for example, you are required to set up user accounts and passwords. Those are things that most people aren't used to doing at home, and it might scare them away".[10]

Although this is clearly a dated example, it provides a good illustration of how average users in days gone by were not expected to be acquainted with security and much of it was simply not seen as their concern. Of course, we are now two decades beyond this, and the technologies and threat landscape of today are both very different. However, while things have clearly moved on a bit since then in terms of the need for users to protect systems from threats that could reach them at home, the users' mindset may not have advanced to the same extent.

Moreover, if we stay with the notion of mindset and think about the psychology of home working, it is easy to imagine how this in itself can serve to introduce further risk. Rather than being in the location that they recognise as the 'workplace', staff are working in the relaxed and safe environment of 'home', and so may be less inclined to feel bound by the policy norms of the workplace.

The impact of the Covid-19 pandemic illustrates where organisations' lack of attention to two of the steps will potentially have let them down and left them vulnerable. As a result, one message is the need to pay more attention to the *breadth* of the 10 steps (which is not really a surprising message, given that all of the steps are part of the recommended baseline anyway).

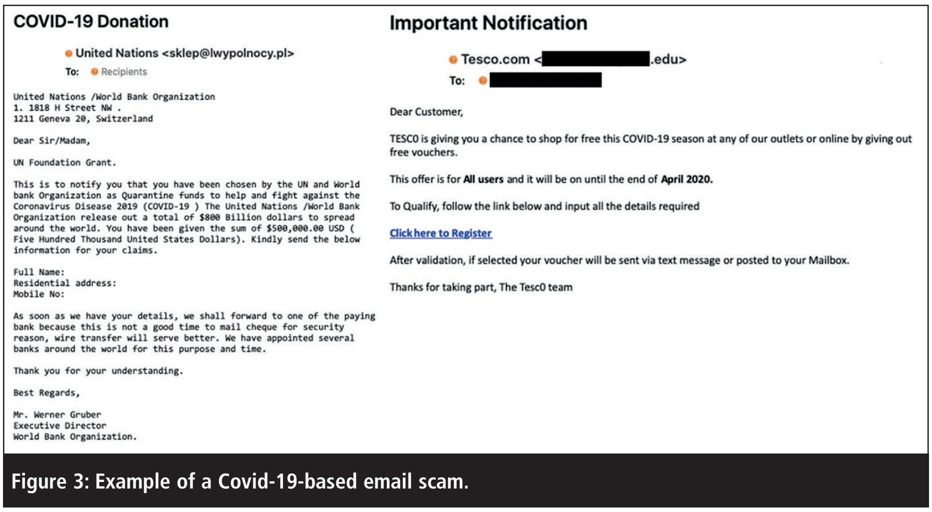
At the same time, there is also a question to be asked around whether businesses that do the 10 steps well in an office environment can do these same steps well when their staff are relocated to home. Those steps that businesses are more likely to have focused on in the workplace setting (eg, secure configuration and network security) may now be less effective, given that people are working outside this environment and relying more upon their own facilities. As a result, all of the expertise and infrastructure that employees had in an office setting risks getting abandoned at home, or at least there is less direct action that IT managers and those in cyber roles can take to prevent people from putting themselves, or the organisation, at risk. Added to this is the problem of what they are now at risk *from*, and the next section illustrates that Covid-19 infection was unfortunately far from the only threat that people needed to safeguard against.

Home and safe?

The Covid-19 context was particularly acute – not only did it increase the dependency on home working (and the associated security provisions to support it), but the pandemic itself also provided a backdrop for an increased level of threat. For example, the period saw particular growth in Covid-19-related phishing and other opportunistic incidents, and the National Cyber Security Centre (NCSC) reported having taken down over 2,000 related online scams during March 2020.[11,12] Meanwhile, findings from (ISC)², based upon a global survey among 256 security professionals, suggested that almost a quarter of organisations had experienced an increase in incidents since moving to remote working, with some reporting that volumes had doubled.[13]

> ***"Individuals were a more vulnerable and easily exploitable target, with fears around the pandemic itself leading them to be concerned, and therefore keen to seek or receive new information about it"***

Findings from the European Network of Cyber Security Centres (ECHO) suggested that attackers' approaches had not changed, but they were provided with a much richer landscape for exploitation. In particular, individuals were a more vulnerable and easily exploitable target, with fears around the pandemic itself leading them to be concerned, and therefore keen to seek or receive new information about it. This in turn led them to be more susceptible to clicking links and downloading files that could turn out to be malicious.[14] In terms of overall scale, findings from Darktrace suggested that the proportion of malicious email traffic targeting home workers rose from 12% in March 2020 (before the start of the UK lockdown period) to over 60% six weeks later.[15]



COVID-19 Donation

United Nations <sklep@lwypolnocy.pl>
To: Recipients

United Nations /World Bank Organization
1. 1818 H Street NW .
1211 Geneva 20, Switzerland

Dear Sir/Madam,

UN Foundation Grant.

This is to notify you that you have been chosen by the UN and World bank Organization as Quarantine funds to help and fight against the Coronavirus Disease 2019 (COVID-19) The United Nations /World Bank Organization release out a total of $800 Billion dollars to spread around the world. You have been given the sum of $500,000.00 USD (Five Hundred Thousand United States Dollars). Kindly send the below information for your claims.

Full Name:
Residential address:
Mobile No:

As soon as we have your details, we shall forward to one of the paying bank because this is not a good time to mail cheque for security reason, wire transfer will serve better. We have appointed several banks around the world for this purpose and time.

Thank you for your understanding.

Best Regards,

Mr. Werner Gruber
Executive Director
World Bank Organization.

Important Notification

Tesco.com <[redacted].edu>
To: [redacted]

Dear Customer,

TESC0 is giving you a chance to shop for free this COVID-19 season at any of our outlets or online by giving out free vouchers.

This offer is for **All users** and it will be on until the end of **April 2020.**

To Qualify, follow the link below and input all the details required

Click here to Register

After validation, if selected your voucher will be sent via text message or posted to your Mailbox.

Thanks for taking part, The Tesc0 team

Figure 3: Example of a Covid-19-based email scam.

As an illustration of the way in which attackers attempted to directly leverage the pandemic, Figure 3 shows two examples of the many Covid-19-themed scam emails circulating during this period, which in this case arrived in inboxes claiming to be from the United Nations and the supermarket Tesco. While neither is particularly special compared to the myriad other email scams regularly doing the rounds, the key point is that they were hooking into the Covid-19 situation as the basis for exploiting their victims, and reaching them on the same systems on which they would be likely to be working from home.

In addition to the human exploitation angle, there has also been significant concern around the vulnerability of the technologies being used to support home working. The most prominent example during the Covid-19 outbreak was Zoom, which initially won praise and plaudits in the early days of home working and lockdown, but soon became the target of significant criticism once security issues started to emerge.[16] While updates were quickly made available to fix the issues, it is easy to imagine some people continuing to use Zoom without updating it (as is the case with much of the other software on self-managed systems). Ultimately, it is again an example of the risk inherent in the rapid switch to the home-based scenario; if remote working was not considered within prior policy and planning then staff found themselves steered toward using a new technology that may have been unfamiliar in itself, and which then proved to have a range of security issues.

Supporting cyber literacy

When looking at the cyber security needs of organisations, many workforce studies and skills surveys tend to focus on cyber security specialists and professionals.[17] However, while these staff are clearly vital in protecting the organisation, they are far from being the full story in terms of cyber security and related skills. In reality, a level of cyber literacy is needed within the workforce as a whole, and not just among those specifically employed with cyber security in their job title.

The Covid-19 situation not only highlighted the need for organisations to support this wider staff base, but also their need to be guided in how to do so. In the UK, the NCSC usefully provided a summary of key issues that organisations should be addressing, supported by related poster and e-learning materials for staff.[18] The NCSC had also already devised a set of 'top tips' for staying secure online, among other new guidance packages around home working, video conferencing and moving business online, which were emphasised and promoted during the Covid-19 lockdown period. While these are by no means a full answer to the issue of secure end-user behaviour, they are certainly a good set of core practices to follow:[19]

- Protect your email by using a strong and separate password.
- Install the latest software and app updates.
- Turn on two-factor authentication on your email.
- Password managers – how they help you secure passwords.
- Secure smartphones and tablets with a screen lock.
- Always back up your most important data.

The NCSC is by no means alone in offering such guidance, and another example was released by the SANS Institute, this time addressing the 'Top 5 steps' for secure home working (addressing the themes of safeguarding the users themselves, protecting their home networks, managing passwords, applying updates, and safeguarding work devices from family and friends).[20]

Even taking just these two examples – NCSC and SANS – it is notable that some of the guidance directly overlaps (eg, around passwords and updates), whereas other points are flagging distinctly different issues (eg, locking mobile devices, taking back-ups and safeguarding work devices are all mentioned by one or other of the guides, but not both). As such, the specific advice that users might get to support their home working endeavours could clearly vary depending upon the source. Furthermore, it is arguable that actually *understanding* what these guides mean and working out how to follow them requires a greater level of cyber security literacy than some users will typically have acquired. Both of these factors point towards the fact that, for best results, organisations ought to be supporting their staff in applying good practice.

Dramatic driver

While Covid-19 provided a dramatic new driver for adopting secure home-working practices, much of the underlying best practice is not new. There is already an abundance of awareness-raising material available, but staff need to be directed towards it and organisations ought to at least be certain that it covers the bases they need to cover.

Of course, there is the question of how much of a priority it would have been for businesses to actually seek out any guidance in the rush to work from home and keep their business running. CSBS 2020 found that only 54% of businesses had sought any external information or guidance on cyber security in the past 12 months. This is higher than it used to be – partly attributable to the General Data Protection Regulation (GDPR) coming into force in 2018 – but it still means that material such as the NCSC guidance does not reach many businesses at all.

"The security aspect of flexible working is an issue that we need to get on top of, as the challenge is only likely to be amplified by future working practices, as well as any economic downturn"

At the same time, the Covid-19 crisis presents opportunities. For example, given that government communication with businesses has been relatively high in recent months due to the uptake of Covid-19-related business-support schemes, these open channels could be further used to help direct businesses toward relevant cyber guidance, progressing what the NCSC is already doing in this space. In the UK context, such advice could, for example, potentially be signposted when a firm searches on GOV.UK for Covid-19 support for businesses. In addition, there could be a wider opportunity to promote cyber guidance via other organisations that businesses turn to in times of crisis (eg, their banks and insurers).

Conclusion

While it was certainly not a situation that anyone welcomed, Covid-19 proved to be a significant catalyst for the adoption of technology-based approaches to flexible working that many would not previously have considered or thought possible for their organisations. At the time of writing, we have yet to see the extent to which this has ongoing or longer-term implications for working practices.

Many organisations will doubtless have seen some benefits, and many will also have seen that they were able to get by with whatever security policy and training they had gone in with (including an absence of it). As such, many are now going to see the enforced home working as having been successful and viable in the longer term, without necessarily having bottomed out the security aspects.

Regardless of Covid-19, the security aspect of flexible working is an issue that we need to get on top of, as the challenge is only likely to be amplified by future working practices, as well as any economic downturn. For example, as we see more people working in the gig economy, they will find themselves operating as 'staff' in multiple organisations, often on a short-term basis. As such, organisations will need to make particular efforts to ensure suitable awareness of the cyber security policies and practices that apply within *their* workplace, so that gig employees can make an appropriate distinction between these and those of other employers for whom they may have been working recently or concurrently.

"When there are multiple organisations and workplaces, achieving a level of basic, workplace-agnostic cyber security literacy is going to be even more important, given that while the specifics may differ, the core principles will be the same"

At the same time, when there are multiple organisations and workplaces, achieving a level of basic, workplace-agnostic cyber security literacy is going to be even more important, given that while the specifics may differ, the core principles will be the same. This will at least help to ensure that employers have a solid foundation to work from in trying to promote their own cultures.

The impacts of Covid-19 are likely to cast a long shadow in many ways. While the issues discussed here clearly pale against the family consequences and loss of life, the fact remains that they will also be long-lasting. When polled on their expectations of effects upon the UK in a year's time, more than three-quarters of the public felt that there would still be ongoing changes to the way we live our lives and the way we work, with a quarter anticipating a great deal of change in each case.[21] If this proves to be the case, then it only underlines the need for the surrounding factors to change and keep pace, so that we can live and work as safely as possible in preparation for the further threats that face us.

About the authors

Steven Furnell is a professor of cyber security at the University of Nottingham. He is also an adjunct professor with Edith Cowan University in Western Australia and an honorary professor with Nelson Mandela University in South Africa. His research interests include usability of security and privacy, security management and culture, and technologies for user authentication and intrusion detection. He has authored over 320 papers in refereed international journals and conference proceedings, as well as books including Cybercrime: Vandalizing the Information Society *and* Computer Insecurity: Risking the System. *Furnell is the current chair of Technical Committee 11 (security and privacy) within the International Federation for Information Processing, and a member of related working groups on security management, security education, and human aspects of security. He is also a board member of the Chartered Institute of Information Security and chairs the academic partnership committee.*

Jayesh Navin Shah is a researcher at Ipsos MORI. He has directed several recent studies focused on the UK cyber security sector and wider tech sector. This includes five waves of the 'Cyber Security Breaches Survey', two cyber sectoral analyses, three waves of research on the UK cyber security labour market and the development of a tool to make it easier for businesses to assess the costs of cyber attacks – all carried out on behalf of the Government's Department for Digital, Culture, Media and Sport (DCMS).

References

1. Furnell, S. 'Securing the home worker'. Network Security, Nov 2006, pp.6-12. Accessed Jul 2020. www.sciencedirect.com/science/article/pii/S1353485806704512.
2. 'Coronavirus Polling – 10-13 April 2020'. Ipsos MORI. Accessed Jul 2020. www.ipsos.com/sites/default/files/ct/news/documents/2020-04/node-658626-659361.zip.
3. 'Region – Business Register and Employment Survey (BRES): Table 3.' Office for National Statistics. 26 Sep 2019. Accessed Jul 2020. www.ons.gov.uk/employmentandlabourmarket/peopleinwork/employmentandemployeetypes/datasets/regionbusinessregisterandemploymentsurveybrestable3.
4. 'Cyber Security Breaches Survey 2020'. Department for Digital, Culture, Media and Sport, 25 Mar 2020. Accessed Jul 2020. www.gov.uk/government/statistics/cyber security-breaches-survey-2020.
5. '10 steps to cyber security'. National Cyber Security Centre, 17 Nov 2018. Accessed Jul 2020. www.ncsc.gov.uk/collection/10-steps-to-cyber security.
6. Pedley, D; Borges, T; Bollen, A; Shah, J; Donaldson, S; Furnell, S; Crozier, D. 'Cyber security skills in the UK labour market 2020 – Findings report'. Department for Digital, Culture, Media and Sport, Mar 2020.
7. Klahr, R; Shah, J; Finnerty, K; Chhatralia, K; Rossington, T. 'Cyber security among charities: Findings from qualitative research'. Ipsos MORI Social Research Institute, Aug 2017. Accessed Jul 2020. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/635593/Cyber_security_among_charities_-_findings_from_qualitative_research_-_DCMS.pdf.
8. Schneier, B. 'On Security Awareness Training'. Dark Reading, 19 Mar 2013. Accessed Jul 2020. www.darkreading.com/risk/on-security-awareness-training/d/d-id/1139381.
9. Ames, A; Stannard, J; Stellmacher, D. 'UK Cyber Survey: Key findings – general public'. Ipsos MORI Social Research Institute, Apr 2019. Accessed Jul 2020. www.ipsos.com/sites/default/files/ct/news/documents/2019-04/uk-cyber security-survey-2019-_slides.pdf.
10. 'Microsoft getting back to business'. Indianapolis Star, 17 Feb 2000, pp.24-25.
11. Donegan, K. 'Coronavirus phishing scams increase amid pandemic's spread'. TechTarget, Mar 2020. Accessed Jul 2020. https://searchsecurity.techtarget.com/feature/Coronavirus-phishing-scams-increase-amid-pandemics-spread.
12. 'Coronavirus: UK forces hundreds of scam Covid-19 shops offline'. BBC News online, 21 Apr 2020. Accessed Jul 2020. www.bbc.co.uk/news/technology-52361618.
13. Mayne. M. 'Half of cybersec staff taken off security, incidents double during pandemic: $(ISC)^2$ study'. SC Media UK, 28 Apr 2020. Accessed Jul 2020. www.scmagazineuk.com/half-cybersec-staff-taken-off-security-incidents-double-during-pandemic-isc2-study/article/1681601.
14. 'The COVID-19 Hackers Mind-set. ECHO White Paper #1, European network of Cyber security centres and competence Hub for innovation and Operations (ECHO), 8 Apr 2020. Accessed Jul 2020.

https://echonetwork.eu/wp-content/uploads/2020/04/20200408-ECHO-WhitePaper-Hackers-Mindset-FINAL.pdf.

15. Jolly, J. 'Huge rise in hacking attacks on home workers during lockdown'. The Guardian, 24 May 2020. Accessed Jul 2020. www.theguardian.com/technology/2020/may/24/hacking-attacks-on-home-workers-see-huge-rise-during-lockdown.

16. Wakefield, J. 'Zoom boss apologises for security issues and promises fixes'. BBC News Online, 2 Apr 2020. Accessed Jul 2020. www.bbc.com/news/technology-52133349.

17. Newhouse, W; Keith, S; Scribner, B; Witte, G. 'National Initiative for Cyber security Education (NICE) Cyber security Workforce Framework'. NIST Special Publication 800-181, National Institute of Standards and Technology, Aug 2017.

18. 'Home working: preparing your organisation and staff'. National Cyber Security Centre, 17 Mar 2020. Accessed Jul 2020. www.ncsc.gov.uk/guidance/home-working.

19. 'Top tips for staying secure online'. National Cyber Security Centre, 17 Dec 2018. Accessed Jul 2020. www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online.

20. 'Top 5 Steps to Securely Work from Home'. SANS Security Awareness, Mar 2020. Accessed Jul 2020. www.sans.org/sites/default/files/2020-03/02-SSA-WorkingFromHome-FactSheet.pdf.

21. 'Future impacts of the Coronavirus on Britain'. Ipsos MORI, 1-4 May 2020. Accessed Jul 2020. www.ipsos.com/sites/default/files/ct/news/documents/2020-05/impact_of_coronavirus_-_economy_lives_work.pdf.

A deep dive into Avivore

Oliver Fay, Context Information Security

Oliver Fay

Until now, most prominent supply chain intrusions have been vertical attacks, with the initial victims typically managed service providers (MSPs) or vendors targeted as a way of getting into and moving up or down the supply chain. However, incidents earlier this year targeting large multi-national firms in the aerospace and defence sectors can best be described as horizontal. Advanced attackers have been leveraging relationships and connectivity between suppliers and partners to get a foothold in each other's value chains.

While investigating these recent supply chain attacks, Context researchers identified a new threat group that they codenamed Avivore.[1] The group was found to be compromising remote connectivity or other collaborative working solutions used by smaller engineering services and consultancy companies in the supply chain to bypass well-defended perimeters and gain access to the main target.

Avivore has been categorised as a previously unknown and untracked nation state-level adversary and the reports into incidents affecting aerospace and defence primes had led to speculation that one of the cyber espionage groups, APT10, the Jiangsu Province Ministry of State Security or JSSD, may be behind them. However, as noted during the investigations, the tools, techniques and processes (TTPs), infrastructure and tooling observed were different from previous campaigns by these groups, so it was possible that it was the work of another, entirely different attacker.

Capable and adaptable

This particular threat group showed itself to be highly capable, adept at 'living off the land', masquerading as legitimate users, as well as forensically covering its tracks. The group demonstrated detailed knowledge of key individuals associated with projects of interest and mirrored the working times and patterns of those users to avoid arousing any suspicions. The attackers were also able to manipulate their victims' environments and security controls in order to facilitate and obfuscate their activities. Examples include modifying firewall rules to accept remote desktop protocol (RDP) over alternate ports and establishing hosts within the victim environment as remote access proxies.

The group's attack methodology for the linked intrusions followed a relatively set format. This was firstly gaining access to the victims through compromised user credentials and legitimate external remote access services, then escalating privileges within the victim environment via the abuse of legitimate tools and/or highly privileged service and enterprise administrator accounts. Next was carrying out account and host enumeration using 'net' commands; scheduling the execution of scripts and a tooling run in the context of the 'SYSTEM' user and then going on to remove forensic artefacts of scripts and tooling; and the clearing of event logs following execution. Finally, the group used RDP for the lateral movement around the victim environment.

Island hopping

Avivore makes extensive use of the infrastructure providing interconnectivity between its victims, a technique referred